[translation]

(19) KOREAN INTELLECTUAL PROPERTY OFFICE (KR)

(12) KOREAN PATENT LAID-OPEN PUBLICATION (A)

(51) Int. Cl.[7]
H04L 12/22

(21) Application No.: 10-2001-0082960
(22) Filing Date: December 21, 2001

---

(71) Applicant: KT Corporation

(72) Inventors: KIM, Cheol-Woo, PARK, Seung-Un, KIM, Sung-Hwan, and KIM, Hyun-Sook
(74) Agent: JEON, Young-Il

---

(54) Title: SYSTEM FOR BACK-TRACKING NETWORK INVADER AND METHOD THEREFOR

**Abstract**

The present invention relates to a system for back-tracking a network invader invading a network and a method therefor. The present invention back-tracks an origination network address of the invader by comparing routers connected to the network of an Internet Service Provider (ISP) with connection sessions of systems which is accommodated in said routers and can be used as a previous path of the invader. The back-tracking system remotely collects the connection session statistical information of the router accommodating a path system, then finds out the previous path system, and repeatedly performs the operation of collecting and comparing this statistical information of the connection session, and thereby finds out the origination address of the invader. The present invention uses that in case of the path system, the routers accommodating the corresponding path system have a pair of connection sessions with the same statistical information. In accordance with the present invention, there is an effect of providing an Internet service which prevents an accident recurrence, is safe, and is reliable by back-tracking the origination address of the invader invading the system of the subscriber network in the ISP provider.

**Representative drawing**

Figure 4

**Index words**

path path, network invader, back tracking, connection session

**Specification**

**Brief description of the drawings**

Fig. 1 is a conceptual drawing of the conventional method of back tracking a network invader.

Fig. 2 is a constitutional drawing of a network including the system of back tracking the network invader in accordance with one embodiment of the present invention.

Fig. 3 is a constitutional drawing illustrated for explaining a back tracking principle of the present invention.

Fig. 4 is a detailed constitutional drawing illustrating the system of back tracking the network invader in accordance with one embodiment of the present invention.

Fig. 5 is a flow chart illustrating the method of back tracking the network invader in accordance with one embodiment of the present invention.

※ Description of mark regarding main parts of the drawings ※

260: Back tracking system
261: Input/output module
262: Router authentication database
263: Back tracking process module
264: Router control module
265: Session checking module
266: Back tracking result database

**Claims**

1. A back-tracking system for finding out an origination system of a network invader by repeatedly performing the action of finding out the previous path system for all path systems, which remotely collects a connection session statistical information connected to a path system from a router accommodating an optional path system under the control by an operator, the system comprising:

an input module being inputted an IP address of a tracing object, an authentication information for accessing said router, and a back-tracking control command from the operator;

a router control module accessing to said router accommodating the IP address of the tracing object inputted through said input module, and then setting up a logging function to a connection session access control list which monitors a packet inputted/outputted to said path system and;

a session checking module finding out a targeted connection session having the same statistic information as the statistic information of the currently tracked connection session from the inputted access control list, when a packet statistic information, a destination address, a reception address, and a packet length information for each connection session of said access control list are inputted from said router;

a back tracking processing module controlling said router control module and the session checking module according to the input/output control command inputted through said input module, finding out said previous path system by using the address of departure of said targeted connection session if said targeted connection session information is inputted from said session checking module, and controlling said router control module and session checking module for the previous path system; and

an output module outputting the state of proceeding of the tracking of said back-tracking process module and the tracking result therefrom.

2. The system of claim 1 further comprising a back tracking result storing module storing the back tracking process result of said back tracking process module by stages.

3. The system of claim 1 further comprising:

a routing process module generating the statistic information of each connection session of said ACL when logging is set up with the ACL from said router control module; and

a connection session statistic transmission module storing the packet statistic information of each connection session of the ACL inputted from said routing process module and transmitting to said session checking module the length of said packet, departure information, and the destination information together with said packet statistic information,

wherein the routing process module and the connection session static transmission module are installed in said router.

2. 4. A back-tracking method for finding out an origination system of a network invader by repeatedly performing the action of finding out the previous path system for all path systems, which remotely collects a connection session statistical information connected to a path system from a router accommodating an optional path system under the control by an operator, the method comprising:

an input step of being inputted an IP address of a tracing object, an authentication information for accessing said router, and a back-tracking control command from the operator;

a router control step of accessing to said router accommodating the IP address of the tracing object inputted through said input module, and then setting up a logging function with a connection session access control list which monitors a packet inputted/outputted to said

path system and;

a session checking step of finding out a targeted connection session having the same statistic information as the statistic information of the currently tracked connection session from the inputted access control list, when a packet statistic information, a destination address, a reception address, and a packet length information regarding each connection session of said access control list are inputted from said router;

a back-tracking processing step of finding out the previous path system by using the address of departure of said targeted connection session if said targeted connection session information is found out at said session checking module, and repeatedly performing said router control step and session checking step for the previous path system; and

a step of recognizing the currently tracking departure address of the connection session as the origination system of said network invader when said targeted connection session is not found in said session checking step.